AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20) ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America

v.

KHALID SIDDIQI,

Defendant.

Case No. 8:22-mj-00565-DUTY

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, the complainant in this case, state that the following is true to the best of my knowledge and belief. On or about the date(s) of August 10, 2022 in the county of Orange in the Central District of California, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 875(c)	Threat by Interstate Communication

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s/
Complainant's signature

NINA VICENCIA, Special Agent, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: August 17, 2022

DOUGLAS F. McCORMICK
Judge's signature

City and state: Santa Ana, California

Hon. Douglas F. McCormick, U.S. Magistrate Judge
Printed name and title

AUSA: B. Marrett (x3505)

A F F I D A V I T

I, Nina Vicencia, being duly sworn, hereby depose and state the following:

BACKGROUND OF AFFIANT

1. I am a Special Agent ("SA") of the Federal Bureau of Investigation ("FBI") and have been so employed since 2010.

2. From 2010 to 2018, I worked numerous counter-terrorism investigations that focused on large networks of terrorist sympathizers and supporters residing in the United States and abroad.

3. In July 2019, I was assigned to work violent crimes and assigned to the Regional Narcotics Suppression Program ("RNSP"), a federally-funded High Intensity Drug Trafficking Area ("HIDTA") task force that consists of the FBI, the Drug Enforcement Administration, the Orange County Sheriff's Department ("OCSD"), the Santa Ana Police Department, and several other local police departments. RNSP is responsible for working crimes committed by Drug Trafficking Organizations ("DTOs"), under Titles 18 and 21 of the United States Code. I have received training in asset forfeiture investigating complex narcotics organizations, and advanced interviewing and interrogation techniques.

4. As an FBI SA, I have participated in numerous search and arrest warrants associated with individuals who were involved in violent criminal acts.

5. Through my investigations, my training and experience, and my conversations with other law enforcement personnel, I have received both formal and informal instruction in investigating violent acts, to include methods and techniques used by criminals to plan, execute, and cover-up their criminal activities.

PURPOSE OF AFFIDAVIT

6. This affidavit is in support of an arrest warrant and complaint charging KHALID SIDDIQI ("SIDDIQI") with a violation of Title 18, United States Code, Section 18 U.S. Code § 875(c) (Threat by Interstate Communication).

7. This affidavit is also made in support of an application for a warrant to search the person, belongings, and containers of SIDDIQI and any digital device found on his person, including but not limited to SUBJECT DEVICE 1, as more fully described in Attachment A, which is incorporated herein by reference; the SUBJECT DEVICES are:

a. Apple iPhone, belonging to SIDDIQI associated with the phone number 949.491.4905, herein referred to as "SUBJECT DEVICE 1"; and

b. Any other digital devices found on SIDDIQI's person at the time this warrant is executed which could contain the evidence, fruits, or instrumentalities described below.

8. The requested search warrant seeks authorization to seize evidence, fruits, or instrumentalities of violations of Title 18, United States Code, Sections 875(c) (Threat by Interstate Communication); 922(g) (Prohibited Person in

Possession of Firearms and Ammunition); and 922(a)(6) (False Statement in Connection with the Attempted Acquisition of a Firearm) (collectively, the "SUBJECT OFFENSES"), as described more fully in Attachment B, which is incorporated herein by reference.

9. The facts set forth in this affidavit are based on my personal observations, my training and experience, and information obtained from other law enforcement officers and witnesses. This affidavit is intended to show that there is probable cause for the requested complaint and does not purport to set forth all of my knowledge or investigation into this matter.

SUMMARY OF PROBABLE CAUSE

10. Title 18, United States Code, Section 875(c) – Threat by Interstate Communication – provides, in pertinent part, that whoever transmits in interstate or foreign commerce any communication containing any threat to injure the person of another, shall be fined under this title or imprisoned not more than five years, or both.

11. This affidavit describes numerous threats that SIDDIQI knowingly made to FBI agents, and others, via law enforcement portals and by other electronic means. In particular, a threat on or about August 10, 2022, an online form submission to FBI NTOC, believed to be sent by SIDDIQI using his cellular telephone (SUBJECT DEVICE 1) while located in the Central District of California stating: "I will kill every single FBI agent that crosses my path in the future! I will murder your

families! I will murder your loved ones! I will murder your relatives! I will murder your entire generation! I will murder every FBI agent on this planet in a single heart beat without hesitation! I will kill you with my bare hands while you have a gun! Fuck your mothers and fathers and president".

12. Nearly all of the threats submitted to NTOC directly or via other governmental agencies originated from an individual identifying themself as SIDDIQI, with a residence in Irvine, California, using an Apple iPhone.

STATEMENT OF PROBABLE CAUSE

A. BACKGROUND ON FBI NATIONAL THREAT OPERATION CENTER

13. The FBI National Threat Operation Center (NTOC) operates 24 hours a day, 365 days a year, providing a mechanism for the FBI to receive potentially critical information, evaluate it, and take appropriate action. In threat-to-life situations, NTOC immediately coordinates with state and local law enforcement partners. In addition, NTOC examines and processes information provided by the public for FBI investigative and intelligence purposes and reports the information to the appropriate field office (FO). As of August 2017, NTOC assumed responsibility for telephone complaint calls from all 56 FOs (as well as most of the resident agencies), the Major Case Contact Center and the Weapons of Mass Destruction tip line. In June 2016, NTOC became responsible for all electronic complaints received by the FBI. NTOC also receives

information from outside local, state, and federal agencies. NTOC is located at 1000 Custer Hollow Road, Bridgeport, West Virginia, 26330.

14. FBI Guardian database is a case management system for handling initial threat information of counterterrorism, counterintelligence, cyber incident, and criminal complaints events and suspicious activity. Guardian allows investigators to track and manage threats and Suspicious Activity Reports during the information collection and lead mitigation period.

15. When NTOC receives information, it is documented in Guardian. A Guardian report containing the information is then passed along to the relevant FO squad for review, follow up, and investigation.

B. THREATS MADE BY SIDDIQI

16. On or about the following dates, except as otherwise noted, an individual who self-identified as SIDDIQI, made the following threats through government agency portals or by other electronic means of communication:

a. On 5/5/2022, SIDDIQI submitted a threat via the OS - Bureau of Diplomatic Security OIG Hotline Intake ("DSS-OIG"), in which SIDDIQI repeatedly stated: "This is how people become mass murderers!" This threat was placed in nearly every fillable field on the form. The Bureau of Diplomatic Security OIG Hotline Intake is located at 1801 Lynn Street, Rosslyn, Virginia.

b. On 03/30/2022, an Anonymous Tipster (identified by the Guardian report as SIDDIQI) submitted an online tip to the FBI NTOC that read: "I'm a victim of terrorism! This is the last message I'm ever going to send you guys!! I'm going after everyone legally, then if that doesn't work, I'm going after everyone with a machinegun.. lock me up or kill me or throw me in a psych ward I don't give a fuck anymore!"

i. In this form submission, in the section requesting the identity of the person(s) engaged in this behavior, SIDDIQI listed the following: United States - Of America, White House, FBI Special Agent Melinda Collins and more. I verified via FBI databases that there is no current FBI employee by the name Melinda Collins. There are ongoing inquiries into whether Melinda Collins was ever previously employed by the FBI or another federal agency.

ii. In addition to recording the text fields inputted by a person submitting the form, NTOC also captures information concerning the digital device used by the submitting person, the potential location of that digital device, and additional metadata. In connection with this tip, NTOC recorded the device information associated with this submission as: "User Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 15_1 like Mac OS X)AppleWebKit/605.1.15 (KHTML, like Gecko) CriOS/98.0.4758.97 Mobile/15E148Safari/604.1." Based on my training and experience

and knowledge of this investigation, I believe that this device is SUBJECT DEVICE 1.

iii. The captured IP address associated with this submission was: "2600:1012:b148:e6c6:39e5:47:3a93:e79f," which, based on open-source information, is an IP address located into New York City. Based on my knowledge of this investigation, I am aware that SIDDIQI previously resided in New York. I also know, based on my training and experience, that it is common for individuals who want their Internet communications to appear anonymous to use virtual private networks (VPNs) to disguise their true IP address.

c. On 7/19/2022, via the FBI NTOC, SIDDIQI submitted a threat: "You are not getting away with what you did to me! I coming after you motherfucking sons of bitchs! Im going to prison or im going to die my way not your way".

i. NTOC captured this submission as originating from IP address "136.52.103.5", via device "Mozilla/5.0 (iPhone; CPU iPhone OS 15_5 like Mac OS X) AppleWebKit/605.1.15(KHTML, like Gecko) CriOS/98.0.4758.97 Mobile/15E148 Safari/604.1". Based on my training and experience and knowledge of this investigation, I believe that this device is SUBJECT DEVICE 1. Further, based on open-source information, the IP address was located in California.

d. On 7/21/2022, SIDDIQI submitted a threat via the FBI NTOC that stated: "The retarded supervisor who conducted

this hate crime operation on me and my family deserves to be put to death! The electric chair! In the next life your ass if mine! Your entire generations asses are mine! Fucking retarded FBI agents who go undercover as California DOJ agents! For what?! I have no criminal history and no criminal record! You want to start street justice and pass judgement? This is why allah aka god calls me the judge? In the next life I will perform street justice and I will pass judgement on everyone! Your asses are mine!100%"

i. NTOC recorded this submission as associated with IP address: "136.52.103.5", which, based on open-source information, was located in California. NTOC also recorded the device associated with the submission as: "Mozilla/5.0 (iPhone; CPU iPhone OS 15_5 like Mac OS X) AppleWebKit/605.1.15(KHTML, like Gecko) CriOS/98.0.4758.97 Mobile/15E148 Safari/604.1". Based on my training and experience and knowledge of this investigation, I believe that this device is SUBJECT DEVICE 1.

e. On 8/10/2022, SIDDIQI submitted a threat via the FBI NTOC that stated: "I will kill every single FBI agent that crosses my path in the future! I will murder your families! I will murder your loved ones! I will murder your relatives! I will murder your entire generation! I will murder every FBI agent on this planet in a single heart beat without hesitation! I will kill you with my bare hands while you have a gun! Fuck your mothers and fathers and president."

i. NTOC recorded this submission as associated with IP Address: "2607:fb91:217:b06d:f8af:e66:f626:92" which, based on open-source information, was located in California. NTOC also recorded the device associated with this submission as a "Mozilla/5.0 (iPhone; CPU iPhone OS 15_5 like Mac OS X) AppleWebKit/605.1.15(KHTML, like Gecko) CriOS/98.0.4758.97 Mobile/15E148 Safari/604.1". Based on my training and experience and knowledge of this investigation, I believe that this device is SUBJECT DEVICE 1.

17. A number of additional submissions made by SIDDIQI to agencies outside of the FBI were received via NTOC. The following are some of those submissions:

a. On August 8, 2022, at 10:01 a.m. Eastern Time, the NTOC received a forwarded email from the Strategic Information & Operations Center (SIOC) regarding a threat to the FBI sent to no-reply@contact.whitehouse.gov from the email address siddiqikyle@yahoo.com.[1] That threat stated: "I will kill every single FBI agent that crosses my path in the future! I will murder your families! I will murder your loved ones! I will murder your relatives! I will murder your entire generation! I will murder every FBI agent on this planet in a single heart beat without hesitation! I will kill you with my

[1] Based on IPD reports with SIDDIQI's contact information and submissions SIDDIQI has made to the FBI, in which he provided his email address, I believe that this is SIDDIQI's e-mail address.

bare hands while you have a gun! Fuck your mothers and fathers and president".

b. An additional submission by SIDDIQI that was received by NTOC on August 8, 2022, at 10:15 a.m. Eastern Time stated the following: "Everyone is Washington is a fucking god dam criminal! I am coming to washing with a motherfucking machine gun and I'm doing this world a favor by shooting up the FBI headquarters! Fuck the FBI and FUCk the United bitch ass state of America! I am now a mass murderer because of you people! I am going to kill people here real soon just watch! Body bags mother fuckers! Body bags and tomb stones!

i. NTOC recorded the IP address associated with this submission as: "2607:fb91:217:b06d:f8af:e66:f626:92", which, based on open-source information, was located in California. NTOC also recorded the device associated with the submission as: "Mozilla/5.0 (iPhone; CPU iPhone OS 15_5 like Mac OS X)AppleWebKit/605.1.15 (KHTML, like Gecko) CriOS/98.0.4758.97 Mobile/15E148Safari/604.1". Based on my training and experience and knowledge of this investigation, I believe that this device is SUBJECT DEVICE 1.

c. On August 8, 2022, at 11:16 a.m. Eastern Time, the NTOC received a second forwarded email from SIOC regarding another threat to the FBI sent to no-reply@contact.whitehouse.gov by SIDDIQI. This threat stated the following: "That bitch ass FBI agent better come out where ever

he is! I'm going to find you mother fucker! 1 min FBI agent! I'm going to make people talk! People will give me your name and address! I'm going to interrogate people with deadly weapons of warfare mother fucker and your family is dead in a ditch! I'm going to kill your entire family bitch nigga! Your ass is mine slice and dice!"

d. On 08/10/2022, at 1:58 AM Eastern Time, another threat came through NTOC regarding threats to the FBI made by SIDDIQI that stated: "I will kill any FBI agent on sight! I don't give a fuck your ass is mine! I will kill you!"

i. NTOC recorded the IP address associated with this submission as: "2607:fb91:217:b06d:f8af:e66:f626:92", which, based on open-source information, was located in California. NTOC recorded the device associated with the submission as: "Mozilla/5.0 (iPhone; CPU iPhone OS 15_5 like Mac OS X)AppleWebKit/605.1.15 (KHTML, like Gecko) CriOS/98.0.4758.97 Mobile/15E148Safari/604.1". Based on my training and experience and knowledge of this investigation, I believe that this device is SUBJECT DEVICE 1.

e. On 08/10/2022, at 6:06 a.m. Eastern Time, SIDDIQI submitted a threat via NTOC that stated the following: "I know everything now! I'm a angrier then ever before FBI agent! God said I'm good! You can't 1 minute me anymore motherfucker! If I see you im going to murder you and anyone else I see that has been plotting against my family and electronicly harassing me

and entrapping me! I live in Irvine California and I shouldn't be dealing with this! Once so ever! I don't need to be dealing with this!"

i. NTOC recorded the device associated with this submission as "Mozilla/5.0 (iPhone; CPU iPhone OS 15_5 like Mac OS X)AppleWebKit/605.1.15 (KHTML, like Gecko) CriOS/98.0.4758.97 Mobile/15E148Safari/604.1". Based on my training and experience and knowledge of this investigation, I believe that this device is SUBJECT DEVICE 1.

18. In the course of this investigation, I also reviewed a screenshot of the Irvine Police Department (IPD) complaint intake system from 8/10/2022. In part, the screenshot showed that IPD received a call from the Central Intelligence Agency (CIA) regarding threatening emails sent to a CIA website. In these emails, SIDDIQI made claims about using firearms against CIA agents as well as FBI agents.

19. On 8/17/2022, I received an email from the California Highway Patrol (CHP) Dignitary Protection Section (DPS) that contained an email from siddiqikyle@yahoo.com that was sent to CHP DPS on 7/12/2022 at 1:37 PM. The email has a header that included the name, "Khalid Siddiqi," the address "228 Duranzo Aisle Irvine CA 92606," and the phone number "(949)491-4905." In that email, SIDDIQI writes: "The FBI doesn't want to help the judge and crown prince because they are trying to murder me…this will start a holy war 100%...this is why they call me the judge

you idiots!!! I get to choose to goes to heaven and hell…everyone is going to hell!!! I will not feel sorry for anyone! This ha been declared before the day the universe was created! 228 Duranzo Aisle Irvine Ca 92606 9494914905".

a. According to the information provided by CHP DPS, this email was attributed to IP address "136.52.103.5".

20. As noted above, on almost every submission to online law enforcement complaint portals, SIDDIQI has self-identified himself as: Khalid SIDDIQI; 228 Duranzo Aisle, Irvine, California 92606; 949-491-4905. Based on open-source information, as well as information provided to me by FBI-TFO Michael Moore, I believe that 228 Duranzo Aisle is SIDDIQI's residence address.

C. SIDDIQI'S PRIOR THREATS TO FAMILY MEMBERS AND DOMESTIC VIOLENCE

21. On or about August 12, 2022, I reviewed a series of IPD reports relating to SIDDIQI. Of those reports, DR 21-11318, and its four supplemental reports, document a domestic violence incident between SIDDIQI and his wife, who is identified in the reports as Jane DOE. The IPD reports span the date range from 9/1/2021 to 11/1/2021 and report an incident in which SIDDIQI grabbed DOE by the neck and began strangling her. After strangling DOE, SIDDIQI then pushed DOE to the floor and dragged her into the closet, where he attempted to close the door on her. This all occurred within feet of the couple's 8-month-old

son, who was in the room when incident occurred. SIDDIQI fled the scene before law enforcement arrived, and DOE was treated by Orange County Fire Authority (OCFA) for injuries sustained to the left side of her head and jaw.

22. The IPD reports further report that although SIDDIQI's mother, Sitara SIDDIQI ("SITARA"), was not present at the time of the incident on the evening of 9/1/2021, SIDDIQI sent her a string of threatening and concerning text messages. I have reviewed screenshots of those messages, several of which appear to have been sent in quick succession as they bear the same timestamp:

a. At timestamp 9:07 PM SIDDIQI sent the following text messages to SITARA:

i. "You and your family and friends and everyone thought it would be funny to ruin mine and my kids lives...I don't give a fuck about Salma[2].. but you took from my kids and you thought it was funny.. if you all don't die and I don't get revenge I promise you that I will kill myself"

ii. "But first I am going after everyone else 1 by 1"

iii. "I don't give a fuck"

iv. "You really pissed me off this time. This is my life's mission!"

[2] As documented in IDP report DR 21-11318, SITARA informed investigators that "Salma" is a nickname that SIDDIQI calls SITARA.

b. At time stamp 9:13 PM, SIDDIQI sent the following text messages to SITARA:

i. "When I see my sons and think about what you all did.. it makes me wanna kill and murder everyone!! I am going to buy a fucking gun and I will do the same thing to everyone including you that you did to me but worse. This is a guarantee! You shouldn't of done it this time and you'll never so this again!!!"

c. At time stamp 1:55 AM on 9/2/2021, SIDDIQI sent the following text messages to SITARA:

i. "I am fighting with everyone and I don't give a fuckkkkk! You are not my mom.. I am going to shoot you and I am going to kill my whole family!!"

ii. "I promise you I don't give a fuck!!"

iii. "You are all dead!!"

iv. "I am buying a gun and I am going to take your fucking life!!"

v. "I am killing everyone!"

23. According to the reports, IPD interviewed SITARA, who stated that this was not the first time SIDDIQI had sent messages threatening his family. She said this was the second or third time this had happened.

D. SIDDIQI'S RESTRAINING ORDERS AND HISTORY

24. I reviewed IPD Report Number: OR-IPD-22-03880-002 regarding a GUN VIOLENCE RESTRAINING ORDER (GVRO) and Search

Warrant for firearms that were obtained by IPD for SIDDIQI. It stated the following:

a. On April 6, 2022, IPD was notified of a threat SIDDIQI made through the United Nations in New York City, via the United States Department of State (DOS) in which he stated that "This is the last message I'm ever going to send you guys!! I'm going after everyone legally then if that doesn't work I'm going after everyone with a machine gun.. lock me up or kill me or throw me in a psych ward I don't give a fuck anymore!"

b. On March 7, 2022 SIDDIQI reportedly told his wife "I'm going to buy a gun and kill everyone....you ruined my life".

c. On March 8, 2022, while speaking to an Orange County Social Worker about an upcoming court hearing SIDDIQI stated, "This is what turns people into mass murderers." The social worker confronted SIDDIQI about the statements, and he claimed he did not make any specific statements about killing anyone and he denied wanting to hurt anyone.

25. Based on CAL-DOJ database searches I conducted, as well as information provided to me by FBI-TFO Moore, I learned that as a result of the domestic violence incident with his wife and the threatening communications with SITARA, the Orange County Superior Court issued an order that SIDDIQI "cannot have custody, control, own, purchase, possess, receive or attempt to purchase any firearm or ammunition including magazines.

Respondent must surrender to a local law enforcement officer or agency all firearms and ammunition including magazines in their custody or control or that they possess or own within 24 hours of receiving this order."

26. In issuing the order, the Orange County Superior Court Judge found that there were "reasonable grounds for the issuance of this order to exist and it is necessary to prevent personal injury to the respondent or other people having custody control, owing, purchasing, possessing or receiving a firearm. Less restrictive alternatives were ineffective or have been determined to be inadequate or inappropriate for the current circumstances."

27. FBI-TFO Michael Moore provided me with a list of cases SIDDIQI currently has pending in Orange County Superior Court. Those cases are as follows:

a. Case Number: 21HF2098 - PC 236 False Imprisonment, PC 245 Assault with a Deadly Weapon, PC 422 Criminal Threats, PC 273.5 Domestic Violence - Inflict Injury on Spouse.

b. Case Number: 21HM04937 - PC 243(e)(1) Domestic Violence on a Spouse or Cohabitant.

c. Case Number: 22HM04067 – PC 273.6 Domestic Violence Restraining Order Violation.

d. Case Number: 22HM05964 – PC 417 Brandish a Weapon, not a firearm.

e. Case Number: 22HM06039 – PC 594 Vandalism

f. Case Number: 22HM06706 – PC 166 Protective Order Violation.

E. SIDDIQI'S ATTEMPT TO PURCHASE A FIREARM APPROXIMATELY ONE MONTH AFTER THREATENING HIS MOTHER

28. On August 13, 2022, I reviewed a State of California Dealer's Record of Sale of Firearm (DROS) report number T2261800979102691. This report reflects that approximately one month after the domestic violence incident and threats described above in Paragraphs –21 and 22, on or about 10/21/2021 SIDDIQI attempted to purchase a 9MM, semiautomatic pistol from Ammo Brothers, located at 1554 Brookhollow Drive, STE B in Santa Ana, California.

29. The status of the transaction is listed as "Denied".

F. SIDDIQI'S POTENTIAL ACCESS TO OTHER FIREARMS

30. On August 13, 2022, I reviewed IPD report number OR-IPD-22-03880-001, which documented the May 18, 2022 execution of a GVRO search warrant at SIDDIQI's residence and evidence found during the search. Based on my review of that report, I learned the following:

a. During the search, one item specified in the warrant was located: a single, unexpended round of 12-gauge shotgun ammunition. The IPD Officer located the item on top of the dresser in a bedroom on the second floor off the residence.[3]

[3] As of the date of this affidavit, investigators are still

31. I spoke with Firearms Specialist FBI Special Agent (SA) Trevor Twitchell regarding the single, unexpended round of 12-gauge shotgun ammunition located at SIDDIQI's residence on May 18, 2022. SA Twitchell informed me that based on his review of a photograph of the ammunition, he was able to make a preliminary determination that the item is ammunition as defined in Title 18, United States Code, Chapter 44, Section 921(a)(17)(A). The ammunition was manufactured by Federal Cartridge Co. in either Minnesota, Idaho, or Missouri, and therefore must have been shipped or transported in interstate or foreign commerce if it was received or possessed in the State of California.

32. In addition to the potential access to firearms demonstrated by the ammunition found within SIDDIQI's residence on May 12, 2022, I also believe based on my knowledge of this investigation that SIDDIQI may have access to firearms through

---

attempting to determine whether the ammunition was possessed by SIDDIQI. While SIDDIQI was known to reside in the residence searched, according to IPD investigators, an individual claiming to be SIDDIQI's roommate later arrived at the Irvine Animal Shelter to retrieve a dog that had been restrained inside the room where the ammunition was found during the search. According to the incident reports I reviewed, IPD investigators also did not locate any shotgun or other firearm capable of firing the ammunition. Although it has not yet been determined whether SIDDIQI possessed the ammunition or a firearm capable of firing the ammunition, the presence of the ammunition in SIDDIQI's residence demonstrates that SIDDIQI potentially has access to firearms and ammunition, even after he was unable to purchase a firearm.

family members. On August 13, 2022, I reviewed a University of Irvine (UCI) Police Department (PD) crime report for case number 22-1334, which documented the execution of a search warrant at the University Student Housing apartment where SIDDIQI's brother HAKEEMULLAH SADDIQI ("HAKEEMULLAH") resided. According to the report, on July 23, 2022, UCI PD obtained the search warrant after HAKEEMULLAH made statements and comments about illegally possessing weapons on campus. During the search, UCI PD found a handgun with a fully-loaded 10-round magazine, three additionally fully-loaded 10-round magazines, one fully-loaded 25-round magazine, one disassembled rifle, and one micro conversion kit. Based on my training and experience, and based on conversations with SA Twitchell, I am aware that a micro conversion kit can be used to easily convert a pistol into a short-barreled rifle by adding a shoulder stock, a rail system, and increased magazine capabilities. Short-barreled rifles have additional restrictions and ATF registration requirements to be legally owned.[4]

33. Based on my training and experience, I know that individuals that have been legally barred from purchasing firearms resort to other methods of obtaining firearms, such as the dark web, illegal gun transfers, assemble or buy ghost guns,

[4] Investigators are still investigating whether SIDDIQI had physical access to his brother HAKEEMULLAH's firearms at any time prior to or after the execution of the UCI PD search warrant.

purchase guns out of state and/or obtained through burglary or theft.

G. SIDDIQI'S ONLINE COMMENTS

34. On 8/8/2022, I received an analysis of open-source social media accounts for SIDDIQ. I reviewed this analysis and observed concerning posts made by SIDDIQI. The analytical review included two personal photos of SIDDIQI. One was a photo of SIDDIQI standing in front of what appears to be a boxing ring. The second photo is a close-up profile photo of SIDDIQI. I know these to be photos of SIDDIQI because I have viewed both his California Driver Licenses photo and his booking photo from his arrest 5/18/2022 with IPD. The following are some of those posts SIDDIQI made from his Facebook account with the account name of Khalid Kyle Siddiqi:

a. On February 14, 2022 at 1:31 PM, SIDDIQI posted an image with the words "People change, even Satan use to be an angel." Along with the image, SIDDIQI wrote "I've got a motherfucking list and you better hope your not on the fucking list! Im going to break everyone I promise!"

b. On February 22, 2022 at 12:47 PM, SIDDIQI posted a photo of what appears to be a fully-automatic Thomas machine gun. With that image, SIDDIQI wrote "The golden gun!"

TRAINING AND EXPERIENCE ON FIREARMS OFFENSES

35. From my training, experience, and the collective experiences related to me by other law enforcement officers who conduct firearms investigations, I am aware of the following:

a. Persons who possess, purchase, or sell firearms generally maintain records of their firearm transactions as items of value and usually keep them in their residence, or in places that are readily accessible, and under their physical control, such in their digital devices. It has been my experience that prohibited individuals who own firearms illegally will keep the contact information of the individual who is supplying firearms to prohibited individuals or other individuals involved in criminal activities for future purchases or referrals. Such information is also kept on digital devices.

b. Many people also keep mementos of their firearms, including digital photographs or recordings of themselves possessing or using firearms on their digital devices. These photographs and recordings are often shared via social media, text messages, and over text messaging applications.

c. Those who illegally possess firearms often sell their firearms and purchase firearms. Correspondence between persons buying and selling firearms often occurs over phone calls, e-mail, text message, and social media message to and from smartphones, laptops, or other digital devices. This includes sending photos of the firearm between the seller and the buyer, as well as negotiation of price. In my experience,

individuals who engage in street sales of firearms frequently use phone calls, e-mail, and text messages to communicate with each other regarding firearms that the sell or offer for sale. In addition, it is common for individuals engaging in the unlawful sale of firearms to have photographs of firearms they or other individuals working with them possess on their cellular phones and other digital devices as they frequently send these photos to each other to boast of their firearms possession and/or to facilitate sales or transfers of firearms.

d. I am also aware that persons who are prohibited from owning a firearm may falsify statements on ATF Form 4473 Firearms Transaction Record in an attempt to lawfully purchase a firearm.

TRAINING AND EXPERIENCE ON DIGITAL DEVICES

36. As used herein, the term "digital device" includes the SUBJECT DEVICES.

37. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files, or remnants of such files, months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data

remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

38. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it can take a substantial period of time to search a digital device for many reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

39. The search warrant requests authorization to use the biometric unlock features of a device, based on the following,

which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. The person who is in possession of a device or has the device among his or her belongings is likely a user of the device. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that

appears to have a biometric sensor and falls within the scope of the warrant: (1) depress Khalid SIDDIQI's thumb- and/or fingers on the devices; and (2) hold the devices in front of Khalid SIDDIQI's face with his or her eyes open to activate the facial, iris, and/or retina-recognition feature.

40. Based on information provided by SIDDIQI and recorded by NTOC, there is probable cause to believe that SIDDIQI submitted threats to the FBI and other government agencies using an Apple iPhone associated with the phone number 949.491.4905.

41. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

///

///

///

CONCLUSION

42. Based on the foregoing, I believe there is probable cause to believe that SIDDIQI violated Title 18, United States Code, Section 18 U.S. Code § 875(c) – Threats by Interstate Communication.

43. I further submit based on the foregoing that there is probable cause to believe that the items to be seized described in Attachment B will be found on the person described in Attachment A.

/s/
Nina Vicencia
Special Agent-FBI

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 17th day of August, 2022.

DOUGLAS F. McCORMICK
HONORABLE DOUGLAS F. McCORMICK

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

PROPERTY TO BE SEARCHED:

This warrant authorizes the search of the person of Khalid SIDDIQI, (DOB: 12/26/1987), as well as any digital device found on his person, in his belongings, or containers, including but not limited to the specific digital device described as an Apple iPhone, belonging to SIDDIQI associated with the phone number 949.491.4905.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 875(c) (Threats by Interstate Communications); 922(g) (Prohibited Person in Possession of Firearms and Ammunition); and 922(a)(6) (False Statements in the Attempted Acquisition of a Firearm) (the "Subject Offenses"), namely:

a. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show call logs, SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the Subject Offenses;

b. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the Subject Offenses;

c. Audio recordings, pictures, video recordings, or still captured images related to the purchase, sale, transportation, or manufacture of guns or ammunition;

d. Audio recordings, pictures, video recordings, or still captured images relating to violent acts against the

agents or employees of the United States, including but not limited to the Federal Bureau of Investigation, or members of SIDDIQI's immediate family.

e. Global Positioning System ("GPS") coordinates and other information or records identifying location on the dates at or near the time communications were sent, made, or received in connection with the Subject Offenses; and

f. Any SUBJECT DEVICE which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

g. With respect to any SUBJECT DEVICE containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

II. SEARCH PROCEDURE FOR DIGITAL DEVICE(S)

3. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

c. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the scope of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to

determine, pursuant to the search protocols, whether the data falls within the scope of items to be seized.

d. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

e. The search team may use forensic examination and searching tools, such as "EnCase," "Griffeye," and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

f. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

g. If the search determines that a digital device does not contain any data falling within the scope of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

h. If the search determines that a digital device does contain data falling within the scope of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

i. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the scope of other items to be seized, the government may

retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

j. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

k. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

4. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

5. During the execution of this search warrant, law enforcement is permitted to: (1) depress SIDDIQI's thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of SIDDIQI's face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

6. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.